SRI VIDYA COLLEGE OF ENGINEERING & TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

QUESTION BANK

Year / Dept / Sem: IV / CSE / 07 **Subject code: CS6551**

Staff Name : M.Mohana **SubjectName: Cryptography and Network Security**

UNIT-I

PART-A

1. **Specify the four categories of security threats.**

   - Interruption Interception
   - Modification Fabrication

2. **Explain active and passive attack with example.**
   Passive attack: Monitoring the message during transmission.
   Eg: Interception
   Active attack: It involves the modification of data stream or creation of false data stream.
   E.g.: Fabrication, Modification, and Interruption

3. **Define integrity and non repudiation.**
   Integrity: Service that ensures that only authorized person able to modify the message.
   Non repudiation: This service helps to prove that the person who denies the transaction is true or false.

4. **Differentiate symmetric and asymmetric encryption?**

Symmetric	Asymmetric
It is a form of cryptosystem in which encryption and decryption performed using the same key. **Eg: DES, AES**	It is a form of cryptosystem in which encryption and decryption Performed using two keys. **Eg:RSA,ECC**

5. **Define cryptanalysis?**
   It is a process of attempting to discover the key or plaintext or both.

6. **Define security mechanism**
   It is process that is designed to detect prevent, recover from a security attack.
   Example: Encryption algorithm, Digital signature, Authentication protocols.

7. **Define steganography**
   Hiding the message into some cover media. It conceals the existence of a message.

8. Why network need security?

When systems are connected through the network, attacks are possible during transmission time.

9. Define confidentiality and authentication

Confidentiality: It means how to maintain the secrecy of message. It ensures that the information in a computer system and transmitted information are accessible only for reading by authorized person.

Authentication: It helps to prove that the source entity only has involved the transaction.

10. Define cryptography.

It is a science of writing Secret code using mathematical techniques. The many schemes used for enciphering constitute the area of study known as cryptography.

11. Compare Substitution and Transposition techniques.

SUBSTITUTION	TRANSPOSITION
*A substitution techniques is one in which the letters of plaintext are replaced by other letter or by number or symbols. ***Eg: Caeser cipher.**	* It means, different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. ***Eg: DES, AES.**

12. Define Diffusion & Cnfusion.

Diffusion:

It means each plaintext digits affect the values of many ciphertext digits which is equivalent to each ciphertext digit is affected by many plaintext digits. It can be achieved by performing permutation on the data. It is the relationship between the plaintext and ciphertext.

Confusion:

It can be achieved by substitution algorithm. It is the relationship between cipher text and key.

13. Define Multiple Encryption.

It is a technique in which the encryption is used multiple times. Eg: Double DES, Triple DES

14. Specify the design criteria of block cipher.

- Number of rounds
- Design of the function F
- Key scheduling

15. Define Reversible mapping.

Each plain text is maps with the unique cipher text. This transformation is called reversible mapping.

16. Specify the basic task for defining a security service.

A service that enhances the security of the data processing systems and the information transfer of an organization. The services are intended to counter security attack, and they make use of one or more security mechanism to provide the service.

17. Define network security.

This area covers the use of cryptographic algorithms in network protocols and network applications.

18. Define computer security.

This term refers to the security of computers against intruders and malicious software.

19. What are hill cipher merits and demerits?

Completely hides single letter and 2 letter frequency information.

20. List-out the types of attack in ceaser cipher.

- Brute force attack.
- Just try all the 25 possible keys.

PART-B

1. Explain the followings:
   (a) Playfair cipher. (8)
   (b) Vernam cipher in detail. (8)
2. Explain simplified DES with example. (16)
3. Write short notes on i) Steganography(16)
4. Explain classical Encryption techniques in detail. (16)
5. Write short notes on
   (a) Security services(8)
   (b) Feistel cipher structure(8)
6. Explain the OSI security architecture. (16)

7. a. Explain various transposition ciphers in detail.(8)
   b. Explain the basic principle of rotor machine. (8)
8. Explain in detail about Feistel cipher with diagram. (16)
9. a.Explain classical encryption techniques with symmetric cipher model. (12)
   b. Explain steganography in detail. (4)
10. Convert "MEET ME" using Hill cipher with the key matrix Convert the cipher text back to plaintext.
11. Write short notes on block cipher modes of operation
12. (i) Discuss any four Substitution Technique and list their merits and demerits. (16)
13. Explain in detail about various types of attacks.
14. Explain in detail about various services provided by X.800.
15. Explain in detail about various Mechanisms provided by X.800.
16. Briefly explain the design principles of block cipher. (8)
17. Write short notes on
    (i)Fermat and Eluer's theorem (8)
    (ii)Chinese Remainder theorem (8)
18. Discuss with neat sketch a network security model. (8)